



ASSEMBLÉE NATIONALE

13ème législature

fichiers informatisés

Question écrite n° 41358

Texte de la question

M. Marc Dolez appelle l'attention de Mme la ministre de l'intérieur, de l'outre-mer et des collectivités territoriales sur les différentes propositions de la Commission nationale de l'informatique et des libertés (CNIL) pour que le fichier du système de traitement des infractions constatées (STIC) soit géré dans le respect le plus strict des dispositions législatives et réglementaires en vigueur. Il lui demande notamment de lui indiquer la suite qu'elle entend réserver à celle visant définir une politique plus stricte de gestion des habilitations et, surtout, des mots de passe qui y sont associés, en particulier, garantir une meilleure confidentialité des mots de passe (tant lors de la remise que de la conservation de ceux-ci) et la mise en place systématique dans chaque service de police judiciaire utilisateur d'un registre permettant de recenser les incidents affectant les connexions au fichier STIC (tentatives de double connexion, perte de mot de passe...).

Texte de la réponse

Les fichiers sont un outil du travail quotidien des services de police et de gendarmerie. Leur utilisation est strictement encadrée, pour garantir la protection des libertés publiques et la confiance de la population vis-à-vis des services publics chargés de protéger sa sécurité. La loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés établit les règles fondamentales (qu'il s'agisse de l'alimentation du fichier, des durées de conservation des données, des droits des particuliers, des contrôles que peut effectuer la commission nationale de l'informatique et des libertés (CNIL) ou encore de l'exactitude des données). Le fichier dénommé système de traitement des infractions constatées (STIC) est soumis en outre à des règles particulières, notamment celle de l'article 21 de la loi du 18 mars 2003 pour la sécurité intérieure, qui prévoit un contrôle du procureur de la République. Pour autant, le rapport récemment publié par la CNIL et les analyses déjà faites par le ministère de l'intérieur ont relevé des insuffisances. Des travaux sont engagés pour perfectionner le fonctionnement de ce fichier. S'agissant de la recommandation de la CNIL tendant à mieux encadrer les modalités de consultation du STIC, et plus précisément de ses préoccupations relatives à la création d'un mot de passe temporaire en cas de perte de mot de passe ou à la suite de trois erreurs consécutives de saisie, il y a lieu de souligner que l'incidence en matière de sécurité est toute relative. Il s'agit en effet d'un mot de passe non définitif, qui ne permet pas directement l'accès aux données, mais qui est simplement destiné à permettre l'obtention d'un nouveau mot de passe définitif. Quant à la mise en place d'un registre local de suivi des changements de mots de passe ou d'anomalies d'accès aux applications, cette suggestion ne serait pas de nature à créer une sécurité supplémentaire significative par rapport aux garanties qui entourent déjà la consultation du STIC. L'accès au STIC est en effet soumis à de strictes conditions et contrôlé. Des textes énumèrent limitativement les catégories de personnels pouvant le consulter, et à quelles fins. L'accès à ce fichier, comme à la plupart des applications de police, s'effectue de surcroît par le portail CHEOPS, dont les règles de fonctionnement permettent de limiter les accès, de maîtriser et de connaître précisément les personnes autorisées à consulter le fichier. La traçabilité des interrogations est assurée et les traces de toute intervention effectuée conservées cinq ans. Des contrôles sont effectués périodiquement par le gestionnaire de CHEOPS, ainsi qu'un suivi statistique du volume de connexions mensuelles, permettant de mener des vérifications a priori sur l'usage des fichiers. Le gestionnaire

de CHEOPS procède en outre à des audits ponctuels et aléatoires sur les connexions. En application de la loi du 6 janvier 1978, la CNIL peut en outre réaliser des contrôles sur place et sur pièce. Lorsque des fonctionnaires utilisent des informations de ce fichier à des fins personnelles et non prévues par les textes, les services d'inspection et, le cas échéant, l'autorité judiciaire, sanctionnent ces dérives, qui sont rares. Pour autant, des progrès sont possibles dans le contrôle de l'utilisation du fichier. Le ministre de l'intérieur a ainsi décidé de développer le recours à la biométrie, qui constituera une garantie scientifique de consultations strictement individuelles et autorisées. Par ailleurs, si le système actuel permet des vérifications a posteriori, il sera souhaitable, lorsque la technologie le permettra, de détecter en temps réel les consultations anormales. Il y a lieu enfin de souligner que le ministre a réactivé dès le mois de septembre 2008 le groupe de travail sur les fichiers de police et de gendarmerie, qui a présenté ses recommandations au mois de décembre. Après une étude approfondie de son rapport, le ministre a annoncé adhérer à l'essentiel des recommandations, dont la mise en oeuvre sera entreprise à partir de cette année, en liaison avec les propositions faites par le CNIL, pour améliorer la saisie, la mise à jour et le contrôle des données figurant dans les fichiers et notamment dans le STIC.

Données clés

Auteur : [M. Marc Dolez](#)

Circonscription : Nord (17^e circonscription) - Gauche démocrate et républicaine

Type de question : Question écrite

Numéro de la question : 41358

Rubrique : Droits de l'homme et libertés publiques

Ministère interrogé : Intérieur, outre-mer et collectivités territoriales

Ministère attributaire : Intérieur, outre-mer et collectivités territoriales

Date(s) clé(s)

Question publiée le : 10 février 2009, page 1237

Réponse publiée le : 21 avril 2009, page 3865